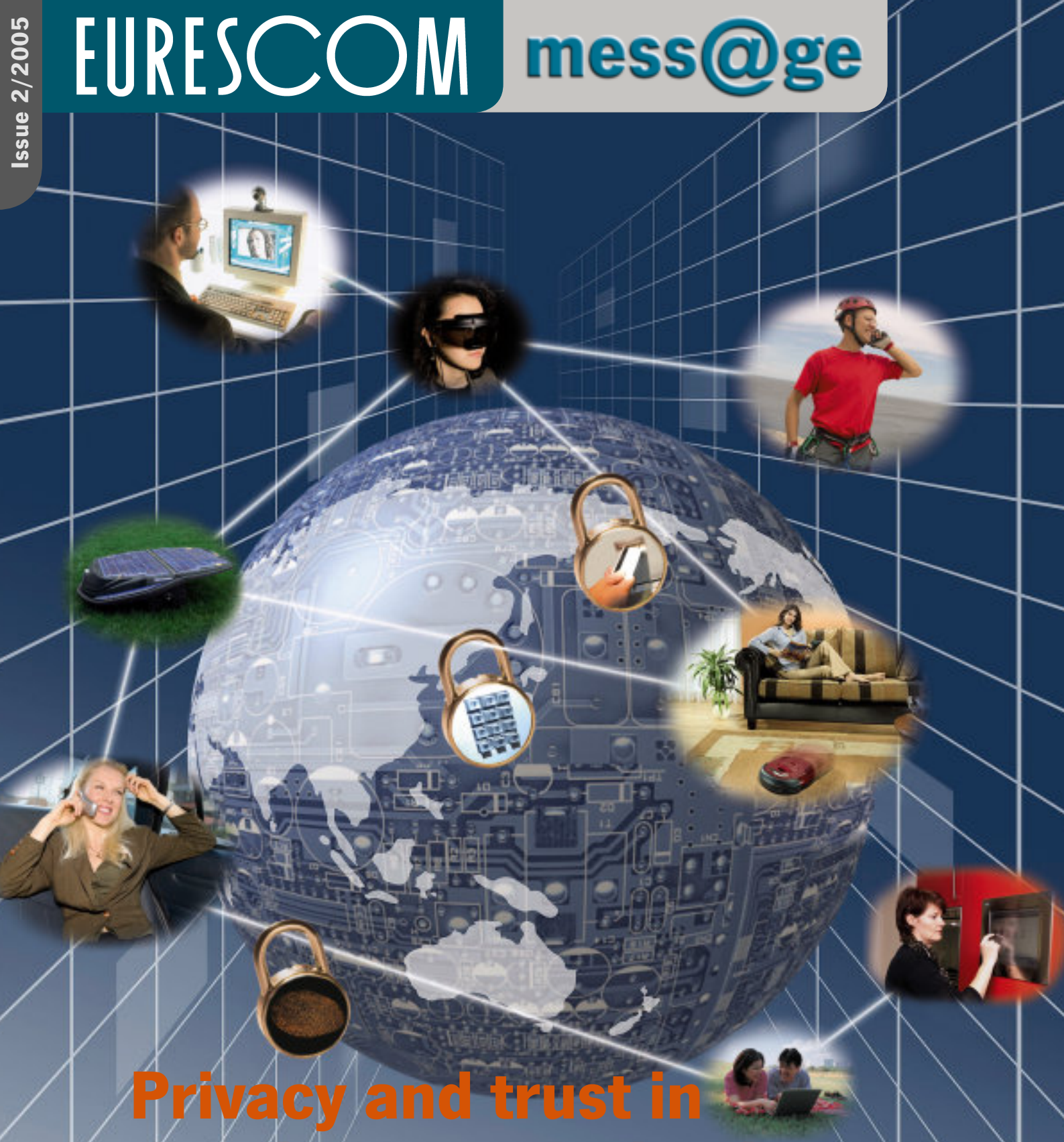
EURESCOM mess@ge
Issue 2/2005



Privacy and trust in pervasive communications

Viewpoint
The digital divide of the elderly

Tutorial
Digital Rights Management

European issues
NEM – The birth of a new industrial sector

Eurescom FP6 proposal and project services

On behalf of its members, major telecoms companies, Eurescom has successfully participated in the EU 6th Framework Programme. Eurescom's unique FP6 services are now also open to other interested companies and institutions.

The scope of Eurescom's FP6 services covers the whole life cycle of a project, from the preparation of project proposals to the implementation of the project and the exploitation of project results.

The Eurescom FP6 services include:

Project preparation

- Feasibility analysis
- Consortium building
- Consortium agreement
- Consortium support
- Proposal writing
- Proposal evaluation

Project implementation

- Project reporting service
- Project website
- Communication and groupware tools
- Administrative support
- Project management

Exploitation of results

- Standardisation input
- Technology transfer
- Workshops & conferences
- Public Relations campaigns
- Training

Please contact us at **info@eurescom.de**, if you are interested to use our services.

Dear readers,

Eurescom mess@ge has a good tradition of picking user aspects and security topics as central themes. Our faithful readers may remember cover themes like "User-focused service development" (issue 4/2002) and "Mobile Security" (issue 4/2001). In this issue we have combined both, user and security aspects. As communications services are growing ever more pervasive, surrounding us permanently wherever we are, the users' trust becomes a decisive factor for the adoption of new services. The trust of users depends to a large extent on the real and the perceived privacy and security they have in a world of ubiquitous communications. We selected some subjects related to privacy and trust, which are currently debated.

One of the communication services that have recently gained huge popularity is Voice over IP (VoIP). Only few users are yet aware of the security risks involved in making phone calls through the Internet. This may change as soon as the first VoIP connections are hacked. Security expert Joachim Posegga gives an overview on the security aspects of VoIP and presents suggestions for making VoIP safer.

Another hot topic at the moment is the use of biometrical data for public security and secure access. *Eurescom mess@ge* author Anastasius Gavras provides information on the current state-of-the-art.

In a number of European countries, there are organisations of concerned citizens who aim to protect privacy rights. *Eurescom mess@ge* talked to Andreas Krisch from European Digital Rights (EDRi) about current privacy issues and his suggestions to resolve them.

However, despite all legitimate concerns about privacy, pervasive communications offers plenty of societal and economic opportunities. The technical and economic aspects of "Ubiquitous Services and Applications" were discussed at the Eurescom Summit 2005 in Heidelberg. See the report in this issue.

There are many more topics covered in this issue, and we hope you will find some of them interesting and useful. We would appreciate your feedback on any of the articles. If you would like to suggest a topic or offer a contribution for *Eurescom mess@ge*, this is equally welcome.

Enjoy reading this issue.

Your
mess@ge editorial team
message@eurescom.de

Events calendar

7 - 8 July 2005

WWRF14 – Future Mobile Device Enablers
San Diego, California, USA
www.wireless-world-research.org

31 August - 2 September 2005

World Information Technology Forum (WITFOR)
Gaborone, Botswana
www.witfor.org.bw

8 - 12 September 2005

IBC 2005 Conference
Amsterdam, The Netherlands
www.ibc.org

25 - 29 September

Gitex 2005
Dubai, United Arab Emirates
www.gitex.com

19 - 21 October 2005

eChallenges e-2005
Ljubljana, Slovenia
www.echallenges.org/2005/

16 - 18 November 2005

World Summit on the Information Society
Tunis, Tunisia
www.smsitunis2005.org/plateforme/

21 - 25 November 2005

27th IDATE International Conference
Montpellier, France
www.idate.org/

30 November - 1 December 2005

Second European Workshop on the Integration of Knowledge, Semantic and Digital Media Technologies (EWIMT)
London, United Kingdom
www.acemedia.org/ewimt2005/

Sn@pshot

Doctor Robot at your bedside

Remotely controlled robots will replace doctors on ward rounds in hospitals, like the St. Mary's Hospital in London (picture). Read more in "A bit beyond" on page 22.

Privacy and trust in ICT
page 7

Ecma International
page 12

Eurescom Summit 2005 in Heidelberg
page 14

Remote presence robots move into hospitals
page 22

Imprint
EURESCOM mess@ge, issue 2/2005 (June 2005)
ISSN 1618-5196 (print edition)
ISSN 1618-520X (Internet edition)

Editors: Milon Gupta (editor-in-chief), Peter Stollenmayer, Anastasius Gavras, Uwe Herzog

Submissions are welcome, including proposals for articles and complete articles, but we reserve the right to edit.
If you would like to contribute, or send any comments, please contact:
Eurescom mess@ge · Schloss-Wolfsbrunnenweg 35 · 69118 Heidelberg, Germany
Tel.: + 49 6221 989 – 123 · Fax: + 49 6221 989 – 209 · E-mail: message@eurescom.de

Advertising: Luitgard Hauer, phone: +49 6221 989 – 405, e-mail: hauer@eurescom.de
Distribution: Eurescom mess@ge is distributed quarterly.

Eurescom mess@ge on the Web:
http://www.eurescom.de/message

© 2005 Eurescom GmbH. No reproduction is permitted in whole or part without the express consent of Eurescom.

+++ News in brief +++ News in brief +++

Diamonds against eavesdroppers

Researchers at the University of Melbourne have developed a technology for making it impossible to eavesdrop on communications or steal information. The new technology is based on a diamond device for improved light transmission through optical fibre.

The Australian researchers developed a device, which generates single light particles that, as they claim, cannot be hacked. They invented a method to grow tiny diamond particles with a size of just 1/1000th of a millimetre onto the tips of optical fibres using a modified, powerful microwave oven. Only diamonds are known to create single photons.

At present, it is possible to divert or tap off some of the billions of light particles, called photons, from a light beam and

James Rabeau, University of Melbourne

reconstruct the information they represent. With the new technology, information is carried on a stream of single photons. Removing any photon would both corrupt the information and break the communication thread. The eavesdropper would end up with no useful information, and the sender and receiver would instantly know they were being bugged.

According to university research fellow James Rabeau, who developed the diamond device, "it is not so much of a problem to have a coded message intercepted, the problem is getting the key." The single-photon beam makes for an unstealable key.

Rabeau and his colleagues received a $3.3 million innovation grant from the Victorian government to develop a prototype device and commercialise the technology.

http://uninews.unimelb.edu.au/articleid_2289.html

Face recognition for mobile phone security

The Japanese automation company OMRON has developed a face recognition technology, which can be implemented in PDAs, mobile phones, or other mobile devices with a camera function. According to OMRON, it is the world's first face recognition technology for mobile phones. The software called "OMRON Vision" is meant to verify the authenticity of the user through face recognition and thus protect the mobile device against data theft.

For registering on his mobile device, the user just has to take his own picture with the device's inbuilt camera. The face recognition sensor will automatically detect the user and unlock the device. The verification process takes less than a second from snapping the photograph. According to

Authentication via photo

OMRON, the software has a recognition rate of 99 percent and is fully compatible to Symbian, BREW, embedded Linux, and ITRON OS.

www.omron.com

Nortel and IBM agree on R&D collaboration

On 20 May, Nortel and IBM announced a joint innovation agreement in the telecommunications market that will focus first on a new class of blade servers. The companies will establish a Nortel-IBM Joint Development Center in Research Triangle Park, NC to collaborate on the design and development of new products and services.

At the Nortel-IBM Joint Development Center, personnel from both companies will work together to enhance and extend current products, collaborate on focused research on a project-by-project basis, and work together on technology, initially, a new class of blade servers. A Nortel spokeswoman said the center will start with 25 to 30 staff, and expand as it tackles new projects

Nortel plans to leverage IBM engineering and technical services for several projects all aimed at extending Nortel's offerings in the areas of fixed and wireless broadband, VoIP, multimedia services and applications. The companies said the joint effort will reduce R&D costs and bring new ideas to the table. Nortel spends more than US$1.5 billion a year on research and is struggling to cut costs.

www.nortel.com/corporate/news/
www-1.ibm.com/press/

Surround sound for headphones

5.1-channel surround sound in Digital Audio Broadcasting (DAB) can now be played back with standard stereo headphones. The Fraunhofer Institute for Inte-

Ensonido

grated Circuits (IIS) developed a new technology called Ensonido, which enables multi-channel sound for headphones in digital broadcasting.

So far, surround sound has been the domain of large loudspeaker set-ups in living rooms or theatres. The Fraunhofer researchers claim that Ensonido now provides nearly the same listening experience through a portable receiver and stereo headphones. In order to play surround sound over stereo headphones, an acoustic model simulates the natural transmission of multi-channel sound from loudspeakers to the human ear.

Multi-channel sound in DAB is achieved by the new "Spatial Audio Coding" technology (SAC). The Moving Pictures Expert Group (MPEG) is currently standardizing this technology as a multi-channel extension of existing perceptual audio codecs.

www.ensonido.com

Privacy and trust in pervasive communications

Introduction to current issues of privacy and trust in ICT

Anastasius Gavras
Eurescom
gavras@eurescom.de

Recent advances in information and communication technologies (ICT) have raised issues of privacy and trust in virtually all areas that are affected by ICT. And you do not have to be an ICT expert to recognise that almost all areas of our lives have, in one way or another, become dependent on ICT.

Due to this importance and the growing pervasiveness of ICT, privacy and trust have become a crucial issue in this domain, being subject to public concerns and controversial discussions.

Informational self-determinism

Generally speaking, privacy is the ability of individuals or groups to self-determine the disclosure and use of information about themselves. The right against unsanctioned intrusion of privacy by the government, corporations or individuals is part of many countries' laws, and in some cases, constitutions. In many cases, individuals voluntarily give up privacy for perceived benefits. An example is the collection of bonus miles for airline passengers. Another example is when an individual is entering an online competition by giving away personal details that are often used for advertising purposes, in order to get a chance to win a prize.

In the telecommunications context the call data records (call destination, call duration) that are used for detailed billing as well as information about connecting to the Internet (online time, IP address) have become subject to public discussion. For several years, law enforcement agencies in various countries have pushed the adoption of data-retention requirements, which would compel communications service providers routinely to capture and archive information detailing the telephone calls, e-mail messages and other communications of their users. In July 2002, the European Union enacted the Directive on Privacy and Electronic Communications (Directive 2002/58/EC) that leaves it to each EU member state to adopt laws authorizing data retention.

The interview on page 11 with Andreas Krisch, board member of European Digital Rights, about the effects of advanced telecommunications services on the users' privacy and trust, provides in-depth insight to the issues at stake.

On the technology side, many developments fuel the worries of citizens about their privacy, notably more in Europe than in the US. Biometric technologies are already commercially used for access control and also at airports for passenger identification and immigration control. More recently, efforts are underway to include biometric data in national ID cards and passports, such as in Germany and the UK. Basic biometric technologies are introduced in the article on page 10.

RFID (Radio Frequency Identification) and, more recently, NFC (Near Field Communication) open up more application fields that certainly can offer benefits for the user as well as business opportunities. Nevertheless, these technologies can be misused: RFID/NFC, for example, can be used to develop behavioural profiles of individuals.

Forced trust

Trust in ICT is an important concept in the sense that a trusted resource is one that you are forced by necessity to trust. The failure of this resource would compromise the function, integrity or security of a system. In security, trust relates much to the degree of confidence one has in the correctness of a function. For example, a company policy trusts the access control at the entrance, so that only eligible persons in possession of a smart card or in knowledge of a PIN code will be granted access to a corporate building.

In telecommunications, the user trusts the operator that he will be presented with a correct bill. At the same time the operator trusts the accounting and billing system to produce correct billing data. The user in this case has no other choice but to trust the operator. Changing the operator does not solve the trust problem for the user. On the other hand, the operator trusts on the ability of technology to function correctly, i.e. provide the wanted service to the user, and also to produce accurate billing data. A wide range of technologies is in place for protecting the telephone and information networks, and also their users, as well as ensuring network availability.

The advent of Internet telephony (VoIP) poses new challenges for the service providers and the users of VoIP.

The article by Joachim Posegga on page 9 explores the risks involved in moving the well-established PSTN voice service to a completely new technology paradigm.

Looking into the future of pervasive systems, in which a significant amount of personalised data will flow through the network, the article on page 8 elaborates on the work of the European project Daidalos towards developing the concepts for building trust and confidence is pervasive systems.

The articles in this cover theme raise a number of controversial issues that are worth to be discussed further. Your feedback on any of these articles would be welcome.

Security and privacy in a pervasive world – The Daidalos approach

James Clarke
Waterford Institute of Technology
jclarke@tssg.org

Christian Hauser
hauser@ikr.uni-stuttgart.de

Martin Neubauer
neubauer@ikr.uni-stuttgart.de
Institute of Communication Networks and Computer Engineering, University of Stuttgart

Daidalos is a European project funded under the Sixth Framework Programme, which aims to integrate a range of heterogeneous networks and to develop pervasive systems on top of them to provide the user with transparent access to personalised communication and information services. Security and privacy are key to the development of such a system. This article addresses some major questions on how to build trust and confidence in pervasive systems where many entities play different roles, mostly for some limited amount of time, and where a significant amount of personal data travel through the network.

Daidalos aims at a platform to allow third party providers to easily deploy pervasive services. As an example of a pervasive service, imagine that you are walking along, watching a video on a handheld device. You enter a room with a large public display, and the video is automatically switched to it, which transparently charges you a couple of cyber-cents. However, this simple example raises a number of important questions. How does the system know that you are entering the room and that you want to use a large display whenever available? How does it know your charging account? How does it know whether you are authorised to use the large display and that the use does not reveal any sensitive data?

The dynamic nature of pervasive systems

Questions like this raise a crucial issue of pervasive systems – privacy and security. It is obvious that such systems will have access to confidential personal information in order to adapt according to the user's personal situation. For achieving privacy, users must be aware of how and where personal data are processed and used. Furthermore, users must be confident that they are interacting with genuine providers.

The dynamic nature of pervasive systems makes these processes even more complicated. While the user is on the move, there will be new services appearing in the vicinity of the user. Moreover, the actual network a user is associated with changes quite often. In addition, it is a widely acknowledged fact that future telecommunication systems will be open to many providers – network, service and content providers. Thus, a user will frequently be confronted with new providers and will have to be authenticated to each of them. Today, trust relationships are static and security settings require significant effort to configure. In a dynamic pervasive system with mobile users – acting also as providers – this is no longer appropriate. As one goal of pervasiveness is to minimise the user's interaction necessary to control the system, Daidalos strives for automation of these processes as far as practicable.

Virtual Identity

For this, a consistent security and privacy framework based on multilateral security is being developed. For achieving privacy protection, the link between a user's identity and his/her personal information must be concealed. However, users must be accountable for their actions. This necessitates the use of pseudonyms rather than anonymity. In Daidalos, we refer to this pseudonym together with the information disclosed in the context of it as a Virtual Identity (VID). A user can have multiple VIDs. These VIDs are controlled by a software component named Privacy Agent, which acts on behalf of and is controlled by the user, implementing the right of informational self-determination.

When a service is first encountered, a privacy policy must be negotiated bilaterally with the service prior to the use. This privacy policy is the basis for a VID of the user's choice, which the service can then use to interact with him/her and access his/her data. Based on the negotiated privacy policy and the chosen VID, the access rights to personal context information are automatically configured. These three building blocks – privacy policy negotiation, identity management and access control to context information – take the burden of understanding the most critical privacy impacts induced by pervasiveness. Moreover, they are taking the necessary configurations away from the user and thus support pervasiveness.

Challenges of the VID approach

There are a number of complex issues that Daidalos is tackling with the VID approach including the protection of the user's VIDs between services, or at least the notification of the user of any VID linking leading to privacy risks. The VID approach has to be supported from the very first stage in design and onwards. Beneath the communication system – including the authentication and authorisation – the VIDs of a user must not be linked whilst being capable of guaranteeing legal enforcement and charging of pseudonymous users.

Another challenge is the effect of the VID approach on the personalisation and user preferences of the pervasive system, which need a substantial effort to build up knowledge about the user's wishes. Compartmentalising the profile into separate VIDs makes it more difficult to identify preferences. Furthermore, if a preference is identified for one VID, it cannot automatically be transferred to any other VID for the same user. This scenario could be confusing to a user who, in general, will not keep track of which preferences have been identified for which VIDs.

Conclusions

Overall, Daidalos presents a sophisticated system approach that will tie different technologies and innovations together in a seamless way with security, privacy, cost, quality of service and efficiency factored into the process. Concerning privacy protection in pervasive environments, it is very important to consider holistic solutions taking into account the application as well as the network, which can be done in Daidalos due to the shared competence of the partners in all those areas. Note that this article can only address one part of the complete Daidalos security and privacy architecture. More details about this part can be found in our paper presented at the Eurescom Summit 2005 [1].

Daidalos is also participating within the Security and Dependability Task Force (www.securitytaskforce.org) set up within the SecurIST project (www.ist-securist.org) in helping to frame the strategic roadmap for security and dependability in Framework Programme 7. The Security Taskforce's goal is to provide Europe with a clear European level view of the strategic opportunities, strengths, weakness, and threats in the area of security and dependability. It will identify priorities for Europe and mechanisms to effectively focus efforts on those priorities, identifying instruments for delivering on those priorities and a coherent time frame for delivery.

Further information about EU project Daidalos is available at *www.ist-daidalos.org*

Reference

[1] J. Clarke, S. Butler, C. Hauser, M. Neubauer, P. Robertson, I. Orazem, A. Jerman Blazic, H. Williams, Y. Yang: "Security and Privacy in a Pervasive World", EURESCOM Summit 2005, Ubiquitous Services and Applications – Exploiting the Potential, Conference Proceedings, 27-29 April 2005, Heidelberg, Germany, VDE Verlag, Berlin, Offenbach (ISBN 3-8007-2891-5), pp. 315-322.

Voice over IP

The end of the world as we knew it

Joachim Posegga
Professor of Security in Distributed Systems, University of Hamburg, Germany
svs-office@informatik.uni-hamburg.de

Should the captain of a cruise ship care about the engine's technology? Certainly, if it matters. VoIP puts the one and only killer application of telcos, voice, on a completely different technology basis. Here is why this matters.

Voice has always been the core service and the cash cow of operators. Technically, voice over ISDN or GSM is tightly coupled to the underlying transport network. Delivering Voice over IP (VoIP) changes this, because the principle underlying the Internet Protocols is the decoupling of network layers.

This principle is an important reason for the tremendous success of the Internet: it replaces monolithic network stacks by loosely coupled layers, and the services are sitting on top. The actual implementation of the individual layers is not even visible, so a service can use any network that provides a compliant interface to services. This results in a dramatic increase of flexibility, in particular since it also decouples services from the innovation cycles of the underlying transport networks.

VoIP implements voice as "just another service" running on TCP/IP. This is probably the biggest challenge "traditional" telecom operators are being confronted with. It seems the Internet revolution in telecommunications is just about to start.

March 2007. You are about to move into a new apartment; do you have to tell your VoIP provider? No, VoIP provides network mobility, so he won't even realize. The DSL connection at the new place is not working? Weird … but the place is cheap, so maybe you should be happy that electricity and water is not cut off. Your new neighbour won't let you use his WLAN until you sorted out the best connectivity option? Strange people here…OK, UMTS is a fall-back, and if you use it sparsely, it will be affordable for a few days. Too bad you cannot use your usual VoIP provider with UMTS, because voice quality is too poor and you are being charged a fortune even for incoming calls.

From a technology point of view, this future scenario is reality. It is left to the imagination of the reader at which point in time it also describes the typical market situation, and what this would meant, e.g. for customer relationship.

Some technical implications of Voice over IP

The standardised way to carry voice over IP consists of the Session Initiation Protocol (SIP) for signalling and RTP for the actual media transfer. Technically, both are certainly not an efficient way for transmitting voice, but this does not matter here. More important are, for instance, the implications to security of VoIP technology, which we will briefly discuss below. At the end of the day, a network operator needs a certain degree of security to justify billing and to prevent fraud. Furthermore, security is a quality of the service offered which protects customers.

The risk involved with VoIP technology is significantly higher than with "traditional" voice networks for the following reasons:

1. **VoIP offers network and device mobility:** Costumers can use VoIP services independently of their access network and the device (client). Mobility, however, makes securing a system much harder: the experience of mobile phones suggests that the only suitable solution is a smart card (SIM), thus a security "footprint" of the service provider in the user's terminal. As of today, VoIP systems do not offer anything like this.
2. **VoIP moves the intelligence from the network into the end points (terminals).** This complicates securing such a system a lot, because a distributed system is much harder to secure than a centralised one. Furthermore, complex, IP-based terminals, as they are needed for VoIP, are an easy target for attacks. Certainly some sort of credentials must be stored in these devices, and experience with viruses and worms in the Internet shows that securing such devices is an uphill battle.
3. Lastly, **the Internet is a "shared medium"**, this means, signalling and payload are accessible to all parties that can access the network. Telco veterans might still remember the reasons for protecting signalling information against end users and third parties. VoIP goes "back to the roots", anyone can send signalling messages unless some sort of protection against it is deployed.

The three security-related issues above just sketch the problem. These issues are elaborated in detail in our paper on VoIP security, presented at the recent Eurescom Summit.

There are, of course, also other technicalities of VoIP that would be worth being considered, for example the problem of localization for emergency calls, or the provision of lawful interception interfaces. All this is beyond the scope of this short article. We chose to focus on security, since this has an obvious relation to billing, and therefore to revenue. Maybe this motivates the captain to consult his chief engineer.

Biometric technologies for secure access

Anastasius Gavras
Eurescom
gavras@eurescom.de

Biometrics is the science and technology for determining the identity of an individual by measuring the person's physiological or behavioural characteristics. Biometric technology can be used to verify that someone is indeed the one who he claims to be. Authentication, i.e. matching a claimed identity with a real identity, together with confidentiality, integrity and availability are the main security related objectives in the information technology context.

There exist three ways to authenticate a person's identity. The first is based on knowledge, i.e. knowing something that no one else knows, such as a pass-phrase, or a PIN (personal identification number). The second is based on possession, i.e. having something that no one else has, such as a key, or a smart card. In both cases an artificial mapping of an identity to a generated code or an issued card is temporarily achieved. The third way to authenticate a person's identity is to evaluate a person's characteristics, such as body attributes or behaviour, i.e. being someone. In the first two cases the risk exists that a person may disclose (code) or loose (card) the security token, while in the third case the security credentials are permanently "attached" to the person. In many cases a combination of the different ways of authentication is used. For example using a smart card usually also requires a PIN code to be entered somewhere.

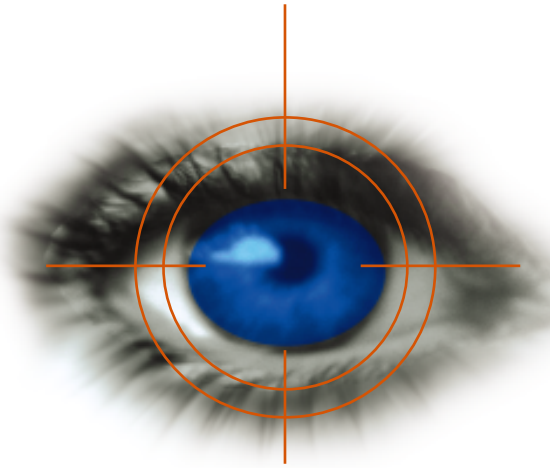
History of biometrics

The first evidence of the use of fingerprints for authentication can be dated back to the time of the early ancient Assyria (about 1900 BC – 1600 BC). Pottery was marked with the potter's fingerprint. In China during the Tang dynasty (618-906) fingerprints were used to sign contracts. Biometrics did not emerge in western cultures until late in the 19th century. The first proposals to use the fingerprint in criminal investigation are dated from 1858. Alphonse Bertillon, a French law enforcement officer and anthropologist, developed an anthropometric system in 1883, which laid the basis for the mass introduction of biometrics use in law enforcement around the world in the beginning of the 20th century.

The technology of biometric systems

In information technology, biometrics refer to technologies for measuring and analyzing human physiological characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements for authentication purposes. Behavioural characteristics that can be measured include signature recognition, gait recognition, speaker recognition, as well as typing (rhythm) pattern recognition.

A biometric system measures a person's biometric data and compares them with pre-registered reference data in order to first identify a person and finally to verify his identity. In a typical system a person registers with the system when one or more of his characteristics are obtained by means of a suitable sensor, processed by an algorithm, and stored in a database. This registration process is called enrolment.



Nobody is perfect

The main technological challenge in biometrics today is the accuracy performance of the biometric system. All human characteristics are subject to change over time and due to temporal conditions. For example, the image of a face may change because of aging; the voice may change during a cold. Also a hand signature never looks the same. The measured biometric data never match 100 percent the reference data. The decision for a "match" or "non match" is thus never concluded on a perfect "equal", but rather depends on the performance parameters of the biometric system. The biometric characteristics are never tested on equality, but only on sufficient resemblance. This means that biometric systems can only identify and verify someone's identity with a certain probability.

The performance of biometric systems is typically measured in terms of the false accept rate (FAR), the false non-match or reject rate (FRR) and the failure to enrol rate (FER). In real-world biometric systems the FAR and FRR can be traded off against each other by changing some parameters. One of the most common measures of biometric systems is the rate at the setting at which both accept and reject errors are equal, known as the equal error rate (EER). The lower the EER, the more accurate the system is considered to be.

Future in biometrics

Despite these deficiencies, biometric systems have the potential to identify individuals with a very high degree of certainty. Currently, the state of the art in forensic DNA evidence enjoys a particularly high degree of trust. The current assumption is that only identical twins have identical DNA. It remains to be seen how practical it could be to use DNA for authentication purposes in information technology. However, substantial claims are being made that iris recognition technology has the capacity to discriminate even between individuals with identical DNA.

Reduce traffic data

Interview with Andreas Krisch from EDRi on privacy in pervasive communications

Andreas Krisch

Communications is becoming pervasive. *Eurescom mess@ge* talked to Andreas Krisch, expert in information systems and board member of European Digital Rights, about the effects of advanced telecommunications services on the users' privacy and trust. European Digital Rights, abbreviated: EDRi, is a civil rights association representing 17 national organisations, which aims to defend civil rights in the information society.

Mr Krisch is also member of the board of the Austrian Association for Internet Users (VIBE!AT), a representative in the Information Society Advisory Council of the Austrian Federal Chancellor, and a delegate to the World Summit on the Information Society (WSIS) where he has participated in the Human Rights Caucus and the Privacy and Security Working Group.

Communications will increasingly surround us wherever we are. How does this influence the users' privacy?

Krisch: While users and economy clearly benefit from the availability of modern means of communications, the developments in communications technology has clearly influenced the users' privacy and will be a key area for privacy protection in the future. In contrast to older technologies which were more location centric, modern communication technologies are highly personalised and record by their very nature lots of privacy sensitive information. This constitutes a potential threat to user privacy.

What are the main challenges to privacy in telecommunications today?

Krisch: The influence of telecommunications on privacy strongly depends on the design and implementation of the technology. Besides the actual communication data, a lot of data is generated which can be used to get insights in the interests and habits of its users. Once recorded it depends on the security and data protection measures applied to which extent the users' privacy is affected by this recording. So it is a key issue of privacy protection to minimise the data generated in the first place, since no data is as secure as data that never was recorded. Modern information technology provides many mechanisms to protect communication: starting with encryption algorithms to protect the content of communications up to mechanisms for making traffic data anonymous in order to keep habits and interests as well as communication partners private. The challenge we face today is to again strengthen the commitment to the communication secret in our society and to translate this commitment into the design of privacy supporting communication technology.

Which factors negatively affect the trust of users and the adoption of telecommunication services?

Krisch: Users are aware that telecommunication services collect lots of data on their private lives. Given this knowledge there are a number of factors that lead to a climate of distrust and promote the impression of pervasive surveillance. Amongst these factors are in-transparent data protection standards of telecommunication companies, data transfers within company networks and data usages for unrelated purposes, but also the increasing demand of law enforcement agencies for access to and retention of traffic data and the transfer of personal data to foreign authorities – as done with flight passenger name records.

There has been a controversial discussion on the use of biometrics. How could security requirements and the protection of the citizens' privacy be harmonised with each other?

Krisch: In recent years security requirements basically translated into increased surveillance and a reduction of data protection. The recent attempts of four member states to enforce mandatory retention of telecommunication data in the EU is an example for that as well as biometric identifiers on RFIDs in EU passports are. All of these measures have a strong drawback: they do not increase security, and it is uncertain whether they increase the ability to find out what happened after a crime was committed. There is no such thing as a secure world. If modern means of communication are under surveillance, criminals will use letters instead. The innocent users of modern communication will have to pay the price by an immense reduction of their privacy. Security can rather be increased by creating a climate of mutual respect, fairness and trust than by mistrust and surveillance.

What has to be done in order to increase the citizens' trust in pervasive communication services?

Krisch: To stick to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which were established in 1980, would be a good start. Especially in terms of use, limitation and reduction of the data collected. Encryption methods should be adopted to secure the content of communication. Traffic data, and the retention thereof, should be reduced to a minimum, and billing systems should be provided that need no recording of single usages. Finally, communication providers should comply with international privacy standards. The best privacy protection are communication technologies that are privacy friendly by design.

The interview was conducted by Milon Gupta. Further information on EDRi is available at www.edri.org

Ecma International
Standards@Internet Speed

Jan W. Van den Beld
Secretary-General of
Ecma International
jan@ecma-international.org

Standardization in information and communication technology and consumer electronics involves special requirements. Short technology life cycles dictate the development time of standards. Ecma International develops "Standards@Internet Speed": Lean, flexible organization allows high-quality standards to be drawn up in less than a year; with the fast-track procedure proposed by Ecma in 1987, an Ecma standard can be approved by ISO or IEC within as little as six months.

Ecma International was established in 1961 on initiative of the heads of three long-standing Europe-based companies – Bull, IBM Europe and ICT – with the objective of eliminating confusion. Since then, Ecma has resolved many working arrangements to become a highly efficient standards-drafting body. So far it has published 363 standards and 88 technical reports. Today it possesses experienced multi-disciplinary staff to guide companies through the maze of international standardization.

Ecma focuses on Information and Communication Technology (ICT) and Consumer Electronics (CE). Current topics include scripting and programming languages, volume and file structures, product safety, environmentally conscious design practices as well as optical and magnetic storage including Holographic Versatile Discs and Cards (HVD & HVC). HVDs' initial capacity of 200 gigabytes – set to grow to 1 terabyte – and high transfer speed – growing from 100 megabits to 1 gigabit per second – represent a quantum leap in storage capacity.

Standardization of leading Ultra-Wideband (UWB) technology

In telecommunications, Ecma deals with architecture, services, protocols, interoperability and management and application aspects of Corporate Telecommunication Networks (CNs). CNs include narrowband and broadband Private Integrated Services Networks (PISNs) and private networks based on the Internet Protocol (IP). A hot topic of standardization at present is Ultra-Wideband (UWB), the leading technology enabling wireless connection of multiple devices for transmission of video, audio and other high-bandwidth data. The communication technology is designed for short-range Wireless Personal Area Networks (WPANs). The combination of broader spectrum and lower power improves speed and reduces interference with other wireless radio systems. The potential and increasing use of UWB are spurring standardization. In April 2005 Ecma founded Task Group 20 (TG20) with the objective of monitoring market developments and defining a standardization strategy. TG20 members are currently working on standardization of the lower levels of the OSI reference model (radio, baseband, media access and control). An Ecma standard is expected to be published by the end of this year.

Next step in Near Field Communication (NFC)

Standardization is also crucial in Near Field Communication (NFC). NFC is a protocol for very short-range communication – distances of up to 10 centimeters – and is optimized for intuitive, easy, secure communication between various devices just by bringing them close together or making them touch. Cards, mobile phones, modems, printers and other peripherals will achieve a new level of interoperability. Next-generation mobile phones will be personal access tokens for payment and other services and will be capable of exchanging payment and other information and even reading smart cards. NFC is backward compatible with the installed contactless cards infrastructure. It can also bootstrap other protocols such as Bluetooth and Wireless Ethernet (WiFi) by exchanging the configuration and session data.

In 2002, Ecma set up Task Group 19 (TG19) to specify the NFC signal interfaces and protocols. In December 2003 the basic standard ECMA-340 and its extension ECMA-352 enabling interoperability with other systems were adopted by the ISO/IEC Joint Technical Committee JTC1. In 2004 Ecma published two more standards defining test methods, which were also approved by ISO and IEC. Task group TG19 is now going one step further and is working on the Near Field Communication Wired Interface (NFC-WI). Here, an analog radio-frequency transmitting and receiving chip is connected via the NFC-WI to a microprocessor handling all the digital processing functions of the NFC protocol. This separation is interesting for mobile phones, among other devices: The radio-frequency unit could be built into the device, and digital processing could be integrated on the SIM card. The Ecma standard specifying this interface is expected out in autumn of this year.

Ecma and ISO: the perfect match

Ecma works closely with other European and international standardization bodies such as ISO, IEC, ITU-T, CEN (European Committee for Standardization), CENELEC (European Committee for Electrotechnical Standardization) and ETSI (European Telecommunications Standards Institute). Although ISO, IEC and Ecma have always enjoyed a natural symbiosis for mutual benefit, their scopes, structures and working methods are very different: Ecma focuses on ICT and CE, while ISO and IEC have far broader scopes; ISO's technical committees work through national bodies, whilst Ecma works directly with industrial companies and non-profit organizations such as universities and government bodies; ISO's five-stage process involves national followed by international consensus-building, where-

as Ecma's members enjoy direct participation in a fast three-stage process. This system enables Ecma to respond to its members' special needs in terms of standardization in ICT and CE. The short life cycles of products such as magnetic and optical storage devices (e.g. DVDs) dictate the development time of standards, which is usually less than a year at Ecma. In addition, software standardization requires an iterative process much akin to that of the release of software products. It is impossible to develop a complete, long-standing standard in a single run.

In the mid 1980s, ISO and IEC created the fast-track procedure based on a proposal by Ecma. After being vetted by Ecma, the standards go through a meticulous international process within JTC1 to ensure quality. Of the 250 fast-track proposals which have been submitted to ISO and IEC to date, Ecma has contributed over 80 percent, only one of which has been rejected. To simplify publication, ISO and Ecma standards are given a very similar structure.

Membership and structure

Ecma has four membership categories with annual fees of 100, 50, 25 and 5 percent of the annual unit value (70,000 Swiss francs during the last six years), which finance the budget, while a reserve fund is available for contingencies.

Ecma's structure consists of two levels: the General Assembly (GA) and the Technical Committees (TCs), which may consist of several task groups depending on their size. The GA is responsible for Ecma's publications, intellectual property rights (IPR), relationships with other organizations, political lobbying with respect to standards relating to environmental issues and product safety, public relations, financing, membership, by-laws and rules. The GA uses qualified votes – e.g. for the approval of publications, which currently amount to 450 – and simple majority votes, e.g. for the creation of a TC. The TCs are responsible for the development of standards and technical reports. Ecma's process ensures high quality and speed. Its members and five-person secretariat proactively pursue the acquisition of new work.

Ecma has secured a strong position

The creation of more than 400 consortia proves that the high-tech industry needs regulating. Ecma and the consortia are complementary, often sharing several members. Ecma combines the agility of consortia with the quality of *de jure* standardization organizations. By linking its efficient infrastructure and proven flexible working methods with well established interfaces to ISO, IEC and other standardization bodies, Ecma has secured a strong position in the standardization of the information and communication technology and consumer electronics industries.

For more information about Ecma International, visit *www.ecma-international.org.*

Viewpoint

The digital divide of the elderly

A huge market lying idle

Peter Stollenmayer
Eurescom
stollenmayer@eurescom.de

For most of us the Internet has become a commodity. Many of us can hardly remember the time when we had to get travel information in a real tourist office, or search for information in one of the 30 printed volumes of Encyclopaedia Britannica. Even birthday and Christmas greetings are increasingly exchanged via e-mail rather than as physical letters. One group of people, however, is left out of this exciting information society world: the large group of elderly people. Whilst according to EUROSTAT 75% of the 15 to 24 year old Europeans use the Internet regularly, the figure decreases to merely 21% for Europeans between 55 and 74 years of age.

If you consider the life situation of elderly people you would think that the opposite should be the case. After finally being retired, there is more time for leisure, travel, private studies, and keeping in contact with family and friends. All activities for which the Internet is an ideal tool.

Why do most seniors not use the Internet?

The main reason, why Internet adoption amongst elderly people is so low, is in my mind very clear: For using the Internet you need to operate a PC, and this is simply too complicated for most elderly people; or at least they think it is. Most of them are not willing to jump over the threshold to learn basic PC skills necessary for accessing the world of Internet applications. According to Seniorwatch, a European Union programme for monitoring the needs and markets for older citizens, 48% of the European citizens older than 50 years agree or strongly agree with the statement "I am too old to familiarise myself with computers". The number increases to 62% amongst the non-PC-users.

Even worse, European seniors feel left alone by politics and industry. Seniorwatch collected information from many elderly people with an abashing result: Only 38% of the European citizens older than 50 years and not using a PC feel sufficiently informed about computers. 48% blame manufacturers not to incorporate their needs in product characteristics.

Is there a market?

First of all the problem is preliminary, and will improve steadily. The generation, for which the use of a PC is as normal as was the use of a typewriter thirty years ago, is growing older and will soon become the older generation. Since the skills to operate a PC are not lost when someone grows older, we can assume that in 10 to 20 years time the Internet usage gap between elderly and younger people will have significantly decreased if not vanished.

Until then, there is a huge unexplored potential market. If we simply assume that we can raise the Internet penetration amongst people older than 55 years from currently 21% to the existing European all-age-group-covering average of 47%, we are talking about a potential market of roughly 35 million people in the enlarged European Union of 25 countries. There are huge regional differences; in Scandinavian countries the usage of Internet amongst the 55+ citizens is higher than 50%, whilst it is less than 10% in southern European countries like Portugal. Nevertheless, the market potential should be large enough for industry to wake up and provide appropriate devices and services.

What can be done?

If we finally accept that:

- older people do not want to be bothered with expressions like "ISDN", "ADSL modem", "Wireless router", "Ethernet", "Windows", "Internet Explorer", etc., nor do they want to learn anything related to these devices and services,
- the main problem is, at least currently, the high threshold of learning how to use a PC,
- another problem is getting a cheap and simple Internet connection at home,

AMD's Personal Internet Computer

we can only solve the issue, if our ICT industry provides a cheap and simple "Internet access device" and a "one-stop, all-inclusive Internet connection service" with a clear and simple tariff structure. Of course, complete installation needs to be included for a moderate lump sum.

I can just not imagine that it is technologically too difficult to develop a simple device for less than 200 euro, which has a button for connecting directly to a simple Internet search portal, a button for sending and reading e-mails in an uncomplicated way, a 9 inch screen as display, a mouse-like device for navigating, a keyboard for typing e-mail texts, and a failsafe function, which automatically returns it into a stable operation mode, should it crash.

I can also not imagine that with all these new ICT service-providing companies on the market, there is none willing to install a one-stop, all-comprising Internet connection at a reasonable all-inclusive tariff. Particularly if we take into account that the potential market could be 35 million people or more just in the European Union.

First steps into this direction are already happening. For example AMD has recently launched its "Personal Internet Communicator" (PIC), a compact device for affordable and simple Internet access, and some Internet service providers have started to offer all-inclusive installations for a flat fee.

More information on European statistics and on the needs of elderly people can be found at:

- *http://epp.eurostat.cec.eu.int/portal/page?_pageid=1090,30070682,1090_30298591&_dad=portal&_schema=PORTAL*
- *http://www.seniorwatch.de/*

More information on the "Personal Internet Communicator" is available at: *http://www.amdboard.com/pic.html*

Ubiquitous services and applications

Eurescom Summit 2005 in Heidelberg

Milon Gupta
Eurescom
gupta@eurescom.de

The Eurescom Summit 2005 in Heidelberg showed from 27 to 29 April the latest R&D trends in "Ubiquitous Services and Applications" that will come to the market in the near future.

At the three-day conference 41 researchers and developers from leading companies in the information and communications sector presented their latest results. The speakers came from 15 countries, including a number of European countries, the USA, Japan, and China. They informed an international trade audience of more than 90 participants about technological advances in areas like ambient networks, mobile peer-to-peer networks, multimodal user interfaces, wearable computers, and personalised communication services. The conference was opened with a keynote speech by

Panel discussion on machine-to-machine communication: Dr. Norbert Streitz, Fraunhofer IPSI, Dr. Dieter Schafhuber, BMW Group Research and Technology, Dr. Fiona Williams Ericsson, and Dr. Volker Reible, Deutsche Telekom (from left).

Dr. Ioannis Chochliouros from OTE speaking on converged service platforms for interactive digital TV in the final session.

Dr. Fiona Williams from Ericsson. She explained the European eMobility technology platform for future research in the mobile and wireless area. On the second conference day, keynote speaker Dr. Norbert A. Streitz from Fraunhofer institute IPSI in Darmstadt, Germany, presented his vision of a communication environment in which computers disappear, because computing and communication capabilities are built into all kinds of everyday objects.

In addition to the technological aspects, the Eurescom Summit also explored the business aspects of ubiquitous services and applications. One of the promising areas is machine-to-machine communication (M-to-M), whose challenges and opportunities were explored in a panel discussion on the second conference day. The panelists Dr. Volker Reible (Deutsche Telekom), Dr. Norbert Streitz (Fraunhofer IPSI), Dr. Dieter Schafhuber (BMW Group Research and Technology), and Dr. Fiona Williams (Ericsson) explored a number of M-to-M topics that have the potential to change business and society in Europe.

Further information about the event is available at
www.eurescom.de/summit2005
where you can also order the DVD-ROM with the streamed presentations from the conference.

The disappearing computer – Dr. Norbert Streitz from Fraunhofer IPSI giving his keynote speech.

Keynote speaker Fiona Williams from Ericsson.

Josef Noll from Telenor demonstrating an innovative RFID application.

Christian Buergy from Wearable Consult presenting a wearable computer.

Service development in the home
Eurescom project OSIAN

Josef Noll
Telenor R&D
Josef.Noll@unik.no

Interesting technologies and devices for homes are appearing on the market, and some early adopters already have them and use them. However, it is still a long way to successful home services for the average user. Satisfying the needs of users living in widely differing household situations cannot be done through a "one size fits all" infrastructure. Having established the user needs and compared them to technology offers, the Eurescom project OSIAN (P1401) suggests to concentrate on service delivery.

While most of the future scenarios either address technology or provide the vision of a distant future, the OSIAN approach focuses on the near future. Some interest groups propose a residential gateway (RG), which is a rather complex and therefore expensive unit. To install such a unit at the customer premises might go beyond the users' willingness to pay and the operators' willingness to invest. The way ahead is to approach the customer through appealing services, based on a rather simple infrastructure.

OSIAN based this near-future vision on the analysis of the existing infrastructure, established from interviews with early adopters. Roughly 80 % of them had two or more PCs in their homes, and 63 % had installed a data network. The majority (80 %) of people who had a data network had it wireless. Addressing the problems with today's infrastructure, 78 % would like to exchange data between PC, TV, and audio equipment, but more than half (55 %) had substantial problems in transferring content around.

Results from the questionnaire were not representative, but provided guidance on what to focus.

Market developments and social trends

The market drivers and trends in the home for 2005/2006 are flat screens and High-Definition TV (HD-TV), broadband recording, either on DVD or on harddisk recorders, and the turn from analogue to digital video and photography. Most important is interconnectivity, established through a media PC or a media center, or simply by carrying your iPod-like device around. The common broadband connection supports always online, as known from the mobile phones, and enables on-demand services. Residential gateways are getting more mature, cheap, and offer services, not just communication. The social drivers of a broadband, always-on connection are on-demand video and multimedia social connectivity. We see a demand for enriched communication in the social context, where "participation in life" becomes easier. Broadband also supports the engagement in virtual interest groups. The home portal becomes the centre for communication, making "my content" available in the house and from outside, and allows the control of the home infrastructure. Users are increasingly aware of the potential services, but the "How to do?" limits service adoption.

Customer expectations towards operator services

Unlike consumer electronics, customers expect from telecom services that they shall work the first time and every time you use them. They should work like the phone does, and not like a PC, which requires "continuous" maintenance. Services shall be easy to handle, they have to work, and they have to be affordable for the customer. Nobody buys a residential gateway. People invest in infrastructure to have access to specific services they need. Thus, an operator has to help the customer from start to end and cannot afford services, which are not working. These services should also be profitable for the operator. These requirements limit the number of selected configurations and support the vision of an easy-to-use customer-care centre.

Infrastructure requirements

In transferring the customer expectations to an infrastructure, we propose a thin gateway with split functionality (figure 1). A thin gateway, which basically acts as an advanced router, will meet the price target of below 100 euro. The split functionality allows both "non supervised" Internet access and secured access to the telecom's service infrastructure. The public access gives the customer the freedom of choice while the secure mode provides access to advanced services with authentication, QoS and remote maintenance, based on functionality in the network.

The secure mode allows (plug &) play applications, as the service components are kept in the network, and home services communicate directly with the centralised service. For the customer, it means just to select a new application, and use it. Secure mode functionality allows the operator to keep control of the service, as the application is kept in the network, and the Quality of Service (QoS) parameters of the home access are controlled by the operator. The advantages are illustrated using video on demand (VoD) provision: Currently customers select a certain access bandwidth, typically in the range of 500 kbit/s to 1.5 Mbit/s. This bandwidth is sufficient for fast Internet access, but only provides limited quality VoD. By moving VoD to the secure mode of the residential gateway, we allow application-based bandwidth, e.g. 2-3 Mbit/s for the video streaming, independent of the limited public access.

Operators' view on service scenarios

OSIAN has identified four main service groups (figure 2), characterised by the most promising service examples and investi-

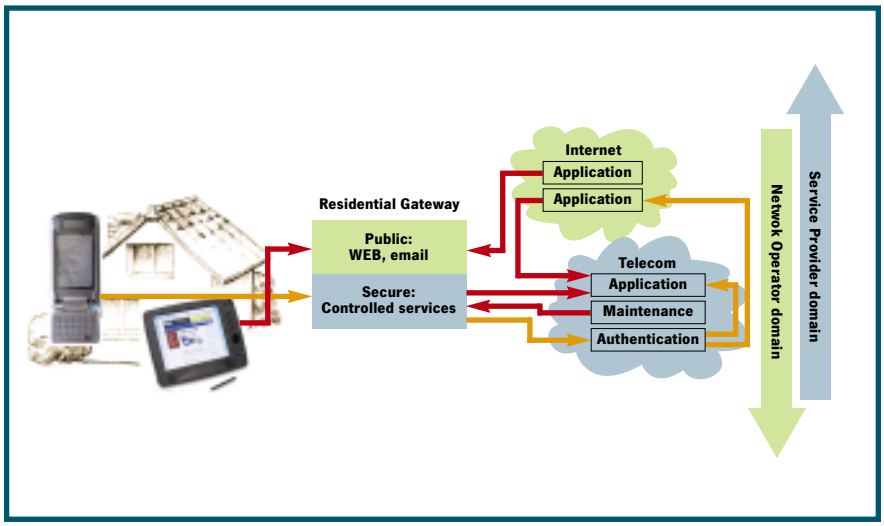


Figure 1: Infrastructure with "split" residential gateway

gated the infrastructure requirements of those services. The service categories are:

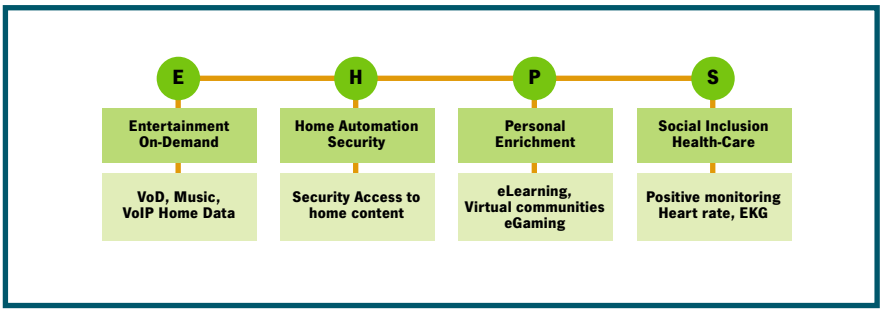


Figure 2: The OSIAN service groups

Entertainment and on-demand services

The **video on demand** example might be extended to all on-demand services and is selected due to the stringent requirements. Characteristic of this type of services is the entertainment aspect, providing users with the information/entertainment exactly when they require it.

The **access to home content** is the second service scenario in the entertainment area. Even though network storage is available, customers tend to keep their pictures/music/videos at home.

This access to home content example demonstrates the value for the customer. It is not the gateway functionality you buy, but the services: network storage and remote access.

Home automation and security

From all home automation services, security surveillance systems had an increase in sales of more than 30 % in Norway in 2004. Today these systems are "closed", with little customer interaction. Customers prefer to see "what is going on at home", including the "baby watch" functionality. This can be enabled by opening access rights to either mobile phones or remote broadband lines.

Personal enrichment

This service covers the **membership in virtual** (interest based) **communities** and eLearning. We selected dancing and do-it-yourself support from hardware stores in order to demonstrate the potential of personal enrichment services.

Social inclusion and health services

This group of services supports participation in the life **across generations**. It covers also positive surveillance, e.g. wireless **monitoring** of health conditions.

Further details on the services and the corresponding infrastructure are available in the project deliverables on the OSIAN website at *www.eurescom.de/public/projects/P1400-series/p1401/*

Conclusion

To achieve successful services is not only a question of responding to technology and service challenges, it is also a question of how to bring the necessary infrastructure into the customer's home. The operators are ideally positioned to integrate the services and bring the infrastructure into the homes. However, current return-on-investment requirements for operators prevent them from rolling out complex and thus expensive infrastructure. The way OSIAN has approached the issue is to provide services over a simple infrastructure, i.e. a thin gateway with split functionality. A thin gateway, which basically acts as an advanced router, will meet the price target of below 100 euro.

The split functionality allows both "non supervised" Internet access and "secured access" to the Telecom's service infrastructure. The public access gives the customer the freedom of choice, while the secure mode provides access to advanced services with authentication, QoS and remote maintenance, based on functionality in the network. The secure mode allows keeping services in the operator's service platform, avoiding the need to update all residential gateways when a new service is introduced. It also enables easy maintenance of the residential gateway, as it is basically an intelligent router. Finally, the secure mode opens up a personalised xDSL access and roaming, allowing customers to use any available wireless home connection, not just their own one. Further studies are necessary to identify the technologies required for secured service provisioning and to establish a roadmap for the introduction of these services.

Digital Rights Management

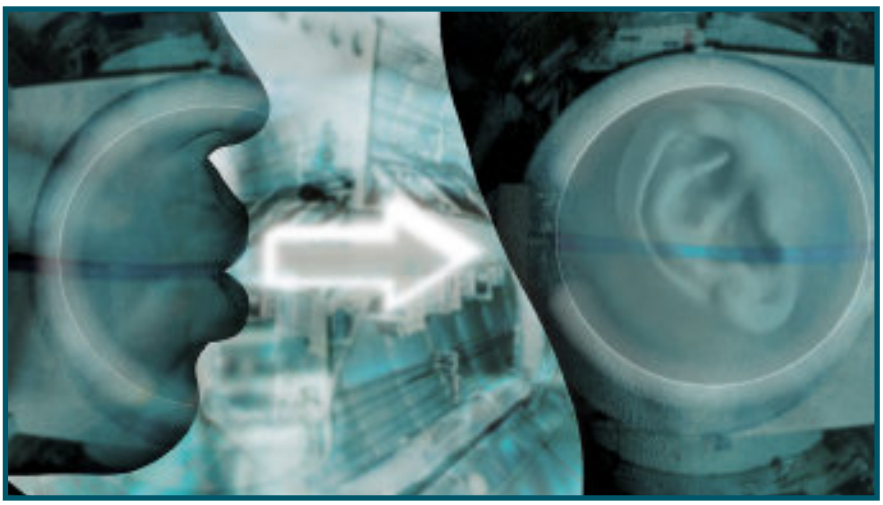
Willem Jonker
Philips Research /
Twente University
willem.jonker@philips.com

Digital Rights Management, or DRM for short, is a much-discussed topic nowadays. The main reason for this is that DRM technology is often mentioned in the context of protection of digital audio and video content, for example to avoid large scale copying of CDs and DVDs via peer-to-peer networks in the Internet. However DRM technology is much more than a simple copy protection technology, it is one of the enabling technologies that will open the way to secure distribution and exchange of digital content over open digital infrastructures such as the Internet.

It is also important to note that DRM is more than technology alone. DRM technology functions in the context of a legal framework that outlines the regulations that DRM technology supports to enforce. Examples of such legal frameworks are privacy laws and copyright laws.

DRM for secure audio and video content management

The secure management of audio and video content is an important application area for DRM. The fact that digital audio and video content can be easily transported



over electronic networks opens the way for electronic delivery of music and movies. Both consumers and content owners are interested in exploiting this new ways of content distribution. For example a networked version of a video rental store would be advantageous to both consumers (that do not need to drive to the rental store) and content owners (that will rent more videos due to a lower threshold). However, in this example there is one issue: how to make sure that the consumer does not watch the video any longer after the rental period is over? Of course this problem also exists with physical distribution, since the consumer can make a copy of the video at home before returning the original to the shop. However, due to the ease of digital content distribution, the impact of such behaviour is much larger in a digital world, something that was clearly demonstrated by the peer-to-peer networks already mentioned before. As a result the development of electronic music and video distribution services is blocked.

In order to show how DRM addresses the problem stated above, we will discuss what DRM technology actually is. There are two main lines of DRM technology based on two different approaches to the problem. The first approach is preventive, while the second approach is reactive.

© Copyright 2004 Apple Computer

Preventive DRM technology

Preventive DRM technology aims at enforcing the legal framework by means of prevention of behaviour that violates the regulations. The technology is based on encryption of the content. The encrypted content can only be accessed through an encryption key. The use of this key is regulated by so called usage rights. A typical electronic distribution system consists of a client-server system. At the server side the content is encrypted and sent to the client. The client needs to be in possession of both the key and the usage right to access the content. The DRM software that runs on the client checks that this is the case.

As an example consider a DRM system that is based on public key cryptography. In public key cryptography we have corresponding key-pairs: a public key Kpu and a private key Kpr. Content that is encrypted with Kpu can only be decrypted with the corresponding Kpr. In such a DRM system each client has its own private key that should be safely stored. The server encrypts content for a specific client using its public key, thus guaranteeing that only this specific client can decrypt the content. The DRM client software checks that the content is used in accordance with the usage rights that have been granted to the client. It is important that the DRM client can be trusted to manage the content according to the usage rules. A client that can be trusted to do so is called a compliant client. Most DRM systems have a so-called revocation method that allows them to distinguish non-compliant clients and block them from receiving content.

Reactive DRM technology

Reactive DRM technology aims at enforcing the legal framework by means of tracing of behaviour that violates the regulations. The approach is also called forensic tracking. The technique that is commonly used is that of embedding information in the content itself that allows tracing the origin of the content. The main technology that is exploited in this context is that of watermarking. Watermarking allows inserting information in music or movies in such a way that consumers do not perceive any difference from the original. It is very difficult to remove or detect a watermark when the characteristics of the watermark are not known. A typical reactive DRM system consists of a server that inserts the watermark containing information on the client at the moment a client downloads content. Violations can be detected by using a watermark detector. Such a detector may, for example, be used to monitor content distribution in the network. If, for example, a usage rule does not allow a client to redistribute the content and the content is nevertheless spotted in the distribution network, the watermark can be used to trace the client that originally downloaded the content.

Standardization and products

There are several activities going on around the standardisation of DRM technology. Important activities are taking place in DVB (Digital Video Broadcasting) for the secure delivery of digital TV, in OMA (Open Mobile Association) for the secure delivery of music and video to mobile phones, in Marlin focussing on efficient implementation of DRM in consumer electronics devices, in Coral focussing on DRM interoperability (i.e. solving the problem of content exchange between different DRM systems), and in MPEG-21 focussing more broadly on the secure exchange of digital items.

Next to standardisation the first proprietary DRM systems are starting to appear, the best known is the Apple iTunes system, but also Microsoft with its Windows Media Technology is offering DRM functionality as well as Sony with its Open Magic Gate system.

DRM in other areas

Although the current application focus of DRM is on secure delivery of music and movies, DRM can be used in a much wider range of applications. It can be used to protect any digital document, and as such it can be used to implement secure workflow systems for example.

Another quite interesting application domain is healthcare. Healthcare has quite strict regulations with respect to privacy of medical data (e.g. HIPAA in the US). At the moment we see a starting digitisation in healthcare. Increasingly, medical information is becoming available in digital form. Already inside hospitals medical information is managed by departmental information systems, and hospital information systems emerge. The next step will be the exchange of medical information between hospitals and all kinds of parties involved in the healthcare processes, leading to the creation of electronic health records containing a lot of privacy sensitive information. DRM technology has the potential of becoming a key technology for the secure exchange of all kinds of medical information.

New director at Eurescom

David Kennedy elected as successor to Dr. Claudio Carrelli by General Assembly

On 11 May, the general assembly of Eurescom unanimously elected David Kennedy as the new director of Eurescom. He will succeed the present director, Dr. Claudio Carrelli, who retires at the end of June.

The outgoing director, Dr. Claudio Carrelli, and his successor, David Kennedy.

David Kennedy has been working for Eurescom since 1997. In 2000 he took over as the senior programme manager responsible for the portfolio of running projects in Eurescom.

Prior to joining Eurescom, the 45 year old from Dublin worked for Irish telecom network operator eircom and their collaborative research subsidiary Broadcom. In addition, he also spent a few years working with Ericsson in Ireland.

Mr Kennedy declared that his goal as the new director is to evolve the company from a membership based collaborative institute into a competitive project management and telecommunications consulting company. "The telecommunications networks and services are becoming increasingly complex and diverse and this brings up greater and greater interoperability and inter-working issues that can only be solved by collaborative initiatives between the key players," he stated.

Explaining the role of Eurescom in this process, Mr. Kennedy said: "Eurescom will identify these issues and, together with the leading industry organisations, establish and manage collaborative projects to solve these issues in a cost-effective way."

The present director, Dr. Claudio Carrelli, has been director of Eurescom since June 1998. Previously, he had worked for 35 years with the Italian telephone operating company, now Telecom Italia, where he served in several positions and responsibilities including R&D, marketing, and international relations.

Throughout his career, Dr. Carrelli has been actively involved in international telecommunications, particularly within the International Telecommunication Union (ITU) and as president of the Information Society Forum, an advisory body to the European Commission on technological and social matters. On retiring, Dr. Carrelli looks forward to being able to spend more time with his family and enjoying his hobbies of golf and sailing.

New Eurescom studies

Three new Eurescom studies on hot issues in the telecommunication area have started. They are briefly introduced below.

Applications and Services for ADSL2+ and beyond (P1551)

Most DSL providers in Europe will soon implement ADSL2 and ADSL2+ in their access networks, offering higher bandwidth to their customers and allowing for a larger distance between customer and ADSL access node as well as lower energy consumption.

This study will look at advanced applications and services, which will make use of such features and might even require higher bandwidth and better QoS than that offered by ADSL2 and ADSL2+. The resulting requirements to enhance the access and core networks of telcos will be analysed as well as the potential impact on service platforms.

The revenue and profit potential for such products will be examined, and a roadmap will be developed to describe an evolutionary way from today's situation to the near future.

For more information contact:
Adam Kapovits, kapovits@eurescom.de

Open Source for Next Generation OSS – issues and challenges (P1552)

Open source software availability and uptake in the area of Operations Support Systems (OSS) is a complex issue and there appears to be a great potential to develop business models that enable standards compliant component implementations, rather than standalone commercial off the shelf (COTS) applications, available to the industry. The study will investigate whether there is any potential for adopting a strategy for the use of open source software for NGN management in the short or medium term future. And if so, it will attempt to develop such an adop-

tion strategy. Furthermore, it will investigate whether open source can satisfy carrier-grade requirements. Finally, the study will elaborate on the long-term impact of open source on OSS systems.

For more information contact:
Anastasius Gavras, gavras@eurescom.de

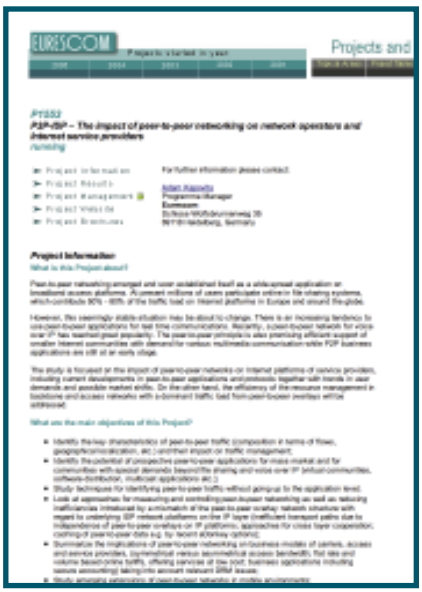
P2P-ISP: The impact of peer-to-peer networking on network operators and Internet Service Providers (P1553)

Peer-to-peer networking emerged and soon established itself as a wide-spread application on broadband access platforms. At present millions of users participate online in file sharing systems, which contribute 50%–80% of the traffic load on Internet platforms in Europe and around the globe.

However, this seemingly stable situation may be about to change. There is an increasing tendency to use peer-to-peer applications for real time communications. Recently, a peer-to-peer network for Voice over IP has reached great popularity. The peer-to-peer principle is also promising efficient support of smaller Internet communities with demand for various multimedia communication, while P2P business applications are still at an early stage.

The study is focused on the impact of peer-to-peer networks on Internet platforms of service providers, including current developments in peer-to-peer applications and protocols together with trends in user demands and possible market shifts. On the other hand, the efficiency of the resource management in backbone and access networks with a dominant traffic load from peer-to-peer overlays will be addressed.

For more information contact:
Adam Kapovits, kapovits@eurescom.de



NEM – The birth of a new industrial sector

David Kennedy
Eurescom
kennedy@eurescom.de

Convergence has been a buzzword in the telecommunications and IT sector for many years now. However, in the recent past it has emerged that there is an even greater convergence challenge to be addressed, and this will affect the way we all live our lives over the next 20 years.

This new convergence is, of course, the convergence between the telecoms/IT world and the broadcasting world. Already there are mobile phones that can receive videos and DVB-H broadcasts. Next there will be seamless interactions between this access and the devices in your home/office, the devices in your hotel room and even the devices in the street. To achieve this model of a comprehensive industrial sector, integrating the best of telecoms, IT and broadcasting, we have to generate an initiative that brings together the leading players from these different communities.

In fact, the new Networked and Electronic Media (NEM) sector comprises of a large variety of industries ranging from the consumer electronics industry, network equipment manufacturers, broadcasters, networks and service providers, content providers, academia, research labs, and related standardisation bodies.

The stakeholders in the NEM sector have a long proven track record of successful collaborative research to achieve large-scale migration to new technologies and market conditions. This allows Europe to maintain the lead on many technological aspects related to this sector, including Digital TV, Digital Video Broadcasting (DVB), and Multimedia Networking.

The heterogeneity of the underlying delivery networks and the difficulties associated to the creation, processing, protection, delivery, presentation, and even regulation of services and content in a convergent landscape has made the development of the NEM sector increasingly complex. In this respect, it faces a number of challenges, risks, and opportunities.

Against this background, the stakeholders have come together to join forces to coordinate future R&D efforts at all levels with a jointly developed Strategic Research Agenda (SRA). First versions of the SRA are available at www.nem-initiative.org but over the next period more and more effort will be put into refining and improving this agenda. The organisations behind this initiative have put forward a proposal to create a Technology Platform that will be a mechanism to present and promote the NEM SRA to the European Community research programmes, national research programmes, and even use it as a basis for global collaboration.

The market size of the NEM sector is estimated to be about 600 billion euro in Europe today. This maintains more than 1.5 million jobs, mostly highly qualified, and therefore is a very significant factor in the economic well-being of many European countries.

Implementing the NEM vision could increase the number of jobs in this area to 3 million by 2015. This means that Europe should make a huge effort to maintain the competitiveness of the sector and take benefit of the enormous opportunities that the NEM sector will offer.

The main objective of the NEM initiative is to foster the development and introduction of novel audiovisual and multimedia broadband services and applications to the benefit of citizens and enterprises, with significant impact on the European economy in the context of the Lisbon objectives. The NEM Initiative is a unique opportunity to bring to all European citizens access to the European cultural diversity.

The focus of the NEM Initiative is on innovative services based on a mix of various media forms, delivered seamlessly and interactively over a variety of complementary access networks to a variety of terminals and devices. It will thereby improve the quality, enjoyment and value of the user experience.

In addition, the NEM Initiative will stimulate worldwide regulations and standardization policies. It will allow EU industry and sector actors to master the required

technologies of the value chain, to develop a consensus on the required standards, to promote international co-operation, and to support the regulatory process.

Within the Eurescom community, France Télécom, BT, Telecom Italia, Telefónica, Deutsche Telekom, and TeliaSonera have already shown their support and commitment to this initiative, and most of them are on the Steering Board of the NEM. Many others are seriously considering it, and we expect that all of our community will at the very least be participants in the General Assembly of the NEM.

Further information is available at *www.nem-initiative.org*

new project results

EURESCOM STUDIES

P1445 OSS for NGN – Co-ordination of telco activities · Deliverable 1 · Recommendations for actions based on the mapping of topics and activities for NG-OSS · Eurescom Study Programme confidential

P1445 OSS for NGN – Co-ordination of telco activities · Technical Information 1 · NG-OSS Topics of the telecommunications industry · Eurescom Study Programme confidential

P1445 OSS for NGN – Co-ordination of telco activities · Technical Information 2 · NG-OSS Topics of the telecommunications industry – Analysis of Industry Activities · Eurescom Study Programme confidential

P1445 OSS for NGN – Co-ordination of telco activities · Technical Information 3 · Recommendations for Actions Based on the Mapping of Topics and Activities for NG-OSS · Eurescom Study Programme confidential

P1447 BISSLA – Business models and Service Level Agreements in open value chains · Deliverable 1
Business models and Service Level Agreements in open value chains · Eurescom Study Programme confidential

P1447 BISSLA – Business models and Service Level Agreements in open value chains · Deliverable 2
Business models and Service Level Agreements in open value chains (presentation) · Eurescom Study Programme confidential

EURESCOM PROJECTS

P1304 CENTS – Cost Effective migration to FTTx-Networks for Tomorrow's Services · Deliverable 2
FTTC Deployment in the Cyprus Telecommunications Authority · Eurescom confidential

P1402 TIMES – The Inter-operator IM and Mobile IM service · Deliverable 1
nalysis of IM Standards, Platforms and their Interoperability · Eurescom confidential

P1402 TIMES – The Inter-operator IM and Mobile IM service · Deliverable 2
Identification and Analysis of IM/Mobile IM business & pricing models · Eurescom confidential

P1402 TIMES – The Inter-operator IM and Mobile IM service · Deliverable 3
IM / Mobile IM business & pricing models (presentation) · Eurescom confidential

P1402 TIMES – The Inter-operator IM and Mobile IM service · Deliverable 4 · IM and Mobile IM Trial · Eurescom confidential

P1402 TIMES – The Inter-operator IM and Mobile IM service · Deliverable 5
Overview of the IM and Mobile IM Trial (presentation) · For full publication

EC PROJECTS

Daidalos Designing Advanced network Interfaces for the Delivery and Administration of Location independent, Optimised personal Services · Deliverable 111 · Consolidated Scenario Description

NM2 new media for a new millennium · The market perspective

CELTIC PROJECT RESULTS

PROMISE Provisioning and monitoring of optical services · Deliverable 2.1 · Definition of optical services and their deployment scenarios

PROMISE Provisioning and monitoring of optical services · Deliverable 3.4 · Requirements for performance monitoring

Robo-doc on ward round

Remote presence robots move into hospitals

Milon Gupta
Eurescom
gupta@eurescom.de

Imagine lying in a hospital bed. Suddenly a robot looking like R2-D2 from Star Wars wheels into your sickroom and says: "How are we feeling today?" This is not science fiction, but reality. In some hospitals in the United States and now also in the UK, robo-docs are making ward rounds.

Doctor Robot is remotely steered by a real doctor via PC and joystick. Instead of a head, the remote presence robot RP6 has an LCD screen on which the face of the remote doctor appears. Two-way video capability enables the doctor to communicate with the patient and zoom in on wounds and charts.

High time pressure on medical staff

One of the first doctors who used the remote presence robot from home is Dr. Louis Kavoussi from Johns Hopkins Hospital, Baltimore, Maryland, where trials have been ongoing since Spring 2004. "Ward-rounds haven't changed since the 1930s – but our hospitals have," Dr. Kavoussi said. "They are bigger now, we have to look after more patients, and sometimes doctors have to cover more than one hospital."

Remote presence robots are meant to fill a critical void. Physicians in hospitals face a growing number of patients who require intensive care. The ageing of the population in most industrialised countries will aggravate this imbalance between a growing number of patients and an overloaded medical staff. Remote presence robots can help physicians and nurses to better cope with the time pressure in medical care.

Remote health control

Critics claim that robots can never substitute the personal touch of a real doctor. High-tech physicians like Dr. Parv Sains, who leads a recently started pilot project at St. Mary's Hospital in London, argue that the benefit of contacting the patient whenever needed outweighs the loss of human touch. "If a specialist is at a conference in California but their medical opinion is needed for a St. Mary's patient, the RP6 robot provides an instant and global link at any time of the day or night," he explained. A major benefit is, according to Dr. Sains, that the doctor who performed a surgery can follow up the healing process of the patient, even if he cannot be physically at the patient's bedside.

Beyond patient care, the robots are also used to remotely consult experts on difficult cases or to allow physicians to attend administrative meetings from outside the hospital.

Another application area could be situations in which it would not be advisable to physically send in doctors, such as in military operations, natural or terrorist disasters, at sea, or in other remote locations.

Popular superhero

The first trials in the US seem to indicate that patients have accepted the robot doctor. "People love it. I was very surprised how much our patients enjoy remote video interactions via the robot," said Dr. Kavoussi. Some patients have even told him that the robo-doc was more enjoyable than a standard bedside visit. At the Hackensack University Medical Center in Hackensack, New Jersey, the robo-doc is called Mr. Rounder and enjoys a particular popularity in the pediatrics wing, where he rolls around dressed in a superhero's cape. "When the robot comes in, everyone giggles," the hospital's chief operating officer, Gwen MacKenzie, was quoted in Business Week.

"Before people see it, they are resistant to the idea," said Yulun Wang, CEO of Californian high-tech startup InTouch Health, who developed the robo-doc. "But once they see that it is just like communicating with a real person, their opinion changes radically."

Further development

In U.S. hospitals the adoption of InTouch's robo-docs is increasing. Thirty-five of them are already making their ward rounds. Customers can rent them for $4,000 a month, or buy them for $120,000 a piece.

InTouch is working on integrating the robot with the hospitals' patient-charting software, so doctors might be able to save streaming-video sequences directly into their patients' electronic charts. The company is also working on a robot that could find its own way from room to room by reading markers on the floor.

Dr. Sains from St. Mary's Hospital does not expect that robots will completely replace doctors on ward rounds. This was confirmed by his medical colleague Dr. Prokar Dasgupta from Guy's Hospital in London, a pioneer in robot-supported surgery: "I like to have some face-to-face contact with my patients."

Further information on the web:
Future of Health Technology Institute
www.fhti.org
InTouch Health
www.intouch-health.com

YOUR AD COULD BE HERE!

Advertising information for Eurescom mess@ge

Eurescom mess@ge delivers up-to-date information on the international R&D activities of Eurescom and solid background information on current research topics in telecoms. The magazine is issued quarterly and available to anyone interested in the development of communications technologies. *Eurescom mess@ge* is sent to subscribers or personally distributed at conferences and workshops. Distributed number of copies per issue: 2,900.

Readers

Eurescom mess@ge has a highly targeted readership. Our readers are international experts and decision-makers from research and other areas of telecommunications and IT. Especially among the members of Eurescom, who are major European telecom network operators and service providers (such as Deutsche Telekom, France Télécom, BT, etc.), *Eurescom mess@ge* has established itself as a major information source on R&D topics.

Advertising rates

In each issue of *Eurescom mess@ge* only two pages are reserved for advertising so that your advertisement receives the maximum attention by our targeted readers.

Inner front cover page or inner back cover page:
Full page: EUR 3,200 (VAT not included)
Half page: EUR 1,600 ((VAT not included)

The advertising deadline for the next issue is 1 September 2005.

Contact for further information and booking advertising space:

Ms Luitgard Hauer, *Eurescom mess@ge*, Advertising
E-mail: hauer@eurescom.de
Phone: +49 6221 989 405
Fax: +49 6221 989 209
Internet: www.eurescom.de/message/

Eurescom mess@ge – The magazine for telecom insiders

EU Project Reporting – Fast and Easy

"Before I had Eurescom Project Reporter, the reporting was cumbersome and it took a long time to get a good overview. Now it is much easier, and I can access the current project data whenever I want. A great tool! However, partners still have to report in time."

Riccardo Pascotto, Deutsche Telekom
Project coordinator of EU Integrated Project DAIDALOS

EU project reporting can be so fast and easy – with Eurescom Project Reporter. Forget about cumbersome, self-made spreadsheet files that have to be uploaded on some server in some directory you always forget. Eurescom Project Reporter offers you an easy-to-use web interface tailored to every partner, which makes entering work and financial data as well as getting a quick overview on the current budget status for EU FP6 Integrated Projects and other EU projects a matter of minutes.

Further information about Eurescom Project Reporter is available at **www.eurescom.de/services**

There you will also find information about our other services for EU/collaborative R&D projects.

Contact us at **projectreporter@eurescom.de**

EURESCOM

European Institute for Research
and Strategic Studies
in Telecommunications GmbH
Schloss-Wolfsbrunnenweg 35
69118 Heidelberg, Germany
Tel.: +49 6221 989-0
Fax: +49 6221 989 209
E-mail: info@eurescom.de
http://www.eurescom.de

Innovation through collaboration

Eurescom is the leading organisation for collaborative R&D in telecommunications. Our mission is to provide efficient management of research projects and programmes for member companies and other clients. We offer more than ten years of experience in managing large-scale distributed R&D using a dynamic network of experts. Companies who wish to collaborate on the key issues facing the telecoms industry are welcome to join the Eurescom community.